ECHOWORX

TECH BRIEF

OneWorld Encryption Delivery Methods Overview

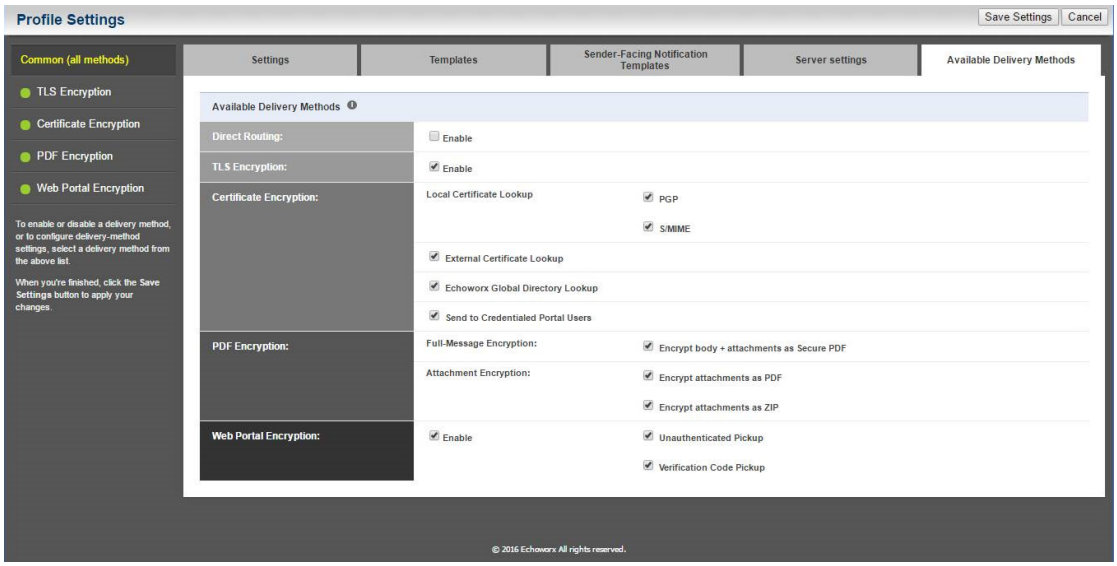
Do you want to communicate securely with business partners? Do you want users to have a seamless experience when sending and receiving encrypted messages?

If you are like most organizations today, you require encryption services for external communications: customers, prospects, and business partners, not just corporate LANs or WANs. The number one reported encryption barrier - asking too much of the email recipients. This indicates that organizations want to deploy email security solutions, without changing the way their employees, customers, and business partners send and receive emails. As an enterprise administrator, you should be able to configure how you want to communicate sensitive information by specifying the method of encryption to use and when to apply it. For instance, you may want to:

- Use no-authentication to securely deliver an email or attachment without any password required;
- Use shared secret to eliminate the need for account registration;
- Deliver a PDF with attachments directly into an inbox.

Echoworx's OneWorld Enterprise Encryption has extensive delivery flexibility; allowing customers to meet a wide range of business use cases and branding requirements. Any or all delivery methods can be used at the same time based on the encryption rule setup. There are unique benefits to each method and based on your business priorities and use cases you will be able to decide which methods are most appropriate.

TLS Encryption | S/MIME Encryption | PGP Encryption | Encrypted PDF Attachment Encryption | Web Portal Encryption



N. America 1 800.346.4193 | UK 44 0.800.368.5334 | Mexico 52 800.123.9553

TLS DELIVERY is extremely easy and seamless for a recipient since they do not have to enter a password to view the message. Recipients receive all messages and data right into their inbox (as clear-text email) without any additional steps.

NOTEWORTHY FEATURES:

- TLS connection is verified for validity on-the-fly.
- Configure a White List (only send to) or Black List (do not send) of TLS domains through web-based admin console.

PROS:

- Senders simply send messages and OneWorld takes care of the rest.
- No need for recipients to change behavior.
- If TLS is not available, auto fall back to other encryption options for delivery (like web portal or Secure PDF).
- Branded footer and header for visibility of security.

CONS:

- If you want messages to stay encrypted at rest, then TLS should not be used.

ENCRYPTED PDF offers the ability to encrypt both body and attachments contained in outgoing email to an Encrypted PDF. The body of the message is encrypted as a PDF page and all attachments are embedded within the single PDF file.

NOTEWORTHY FEATURES:

- Self-Registration: Recipient gets one-time registration message to set their own password
  - Registration can also include out-of-band confirmation (on registration).
  - Authentication can be through existing bank portals (no URLs). Customer logs in to existing portal and through webservice calls is auto-logged into PDF password management portal.
- Sender Set Password: Recipient provides password the sender set at time of sending through the plugin or through subject line trigger.

PROS:

- Excellent mobile experience.
- Complete branded experience for recipient including all customer facing webpages, encrypted messages, and email notifications.
- Deliver encrypted PDFs right to a recipient's inbox.
- Message is encrypted at rest.
- Ability to save messages locally and view offline.
- Ability for passwords to be set by the sender or by the recipient.
- Secure reply functionality.
- Recipient can use any standard PDF viewer on any device to open up the encrypted PDF.

CONS:

- Limited message tracking.
- No read receipt option for sender.

ENCRYPTED ATTACHMENT is beneficial in cases when an organization wants to deliver attached confidential documents without sensitive information in the body of the email. This option is commonly used by applications that generate and process bulk electronic statements.

NOTEWORTHY FEATURES:

- Original PDF attachments remain unchanged, and encryption is applied
- Other Attachments are placed in a Secure PDF or Secure ZIP container
- Self-Registration (same as Encrypted PDF)
- Sender Set Passwords (same as Encrypted PDF)
- Branded header and/or footers added to the message body with Account Management link or Shared Secret Hint

PROS:

- The message body is clear-text when there was no need to encrypt it.
- Excellent mobile experience.
- Complete branded experience for recipient including all customer facing webpages, encrypted messages, and email notifications.
- Deliver encrypted PDFs right to a recipient's inbox.
- Message is encrypted at rest.
- Ability to save messages locally and offline.
- Ability for passwords to be set by the sender or by the recipient.

CONS:

- No secure reply option (but this is desirable when sending address is a "no-reply" mailbox).
- For Secure ZIP, recipient must have ZIP software installed capable of opening AES 256-bit files (such as WinZIP, SecureZIP, WinRAR, 7-ZIP).
- Limited message tracking.
- No read receipt option for sender.

CERTIFICATE ENCRYPTION is beneficial when recipients already have a 3rd party S/MIME or PGP key.

NOTEWORTHY FEATURES:

- Certificate Encryption based on user uploaded public certificate.
- External lookup in LDAP for public recipient certificate.
- Full PGP key creation / management for senders to external PGP users. External users will get a PGP encrypted email that is a digitally signed, and public key attached for the sender. Eliminates need for PGP desktop software under PGP communication.

PROS:

- Upload existing keys to OneWorld.
- Auto generate new keys as needed, maintaining current and future identities.
- No need for recipients to change behavior.
- Delivery can be made to any email address in the world (assuming key exists).

CONS:

- Configuration of inbound email flow is required to detect encrypted reply messages.

WEB PORTAL ENCRYPTION enables delivery of encrypted messages via a secure website. The email is not delivered to the recipient, but instead users are notified in their regular Inbox that an encrypted email is waiting for them.

NOTEWORTHY FEATURES:

- Self-Registration: Recipient gets one time registration message and registers and set their own password
  - Registration can also include out-of-band confirmation (on registration).
  - Authentication can also be through OAuth connectors.
  - Authentication can be through existing bank portals (no URLs in notifications).
- No-Authentication: Recipient gets a URL that directly opens the message (no registration).
- Sender Set Password: Recipient enters a password the sender set at time of sending through the plugin or through subject line trigger.
- Out of Band Password: System generates per message password and emails back to sender. Recipient must obtain system password out-of-band from sender to gain access to message.

PROS:

- Excellent mobile experience.
- Complete branded experience for recipient including all customer facing webpages, encrypted messages, and email notifications.
- Message is encrypted at rest.
- Ability to save messages locally.
- Ability for passwords to be set by the sender or by the recipient.
- Secure reply functionality.
- Read receipts.
- Full message audit for both sender and Adminstrator.
- Message recall for both sender and Administrator.

CONS:

- Retention period (30, 60, 90 days) then deleted.
- Recipient must leave their local mailbox to retrieve messages online.

Since 2000, Echoworx has been bringing simplicity and flexibility to encryption. Headquartered in North America and with offices in the UK, our certified, redundant and replicated data centres are located in the US, UK and Canada. Our passionate encryption experts transform chaos into order for world leading enterprises and OEM providers who understand the requirement for secure communication is of the upmost importance. We are proud to have clients in 30 countries worldwide, with more than 5,000 enterprise-level deployments.

Encryption is an investment in brand, maximizing competitive advantage.

Echoworx's flagship solution, OneWorld Enterprise Encryption, provides an adaptive, fully flexible approach to encryption that ensures the privacy of sensitive messages. Enterprises investing in Echoworx's OneWorld platform, are gaining an adaptive, fully flexible approach to encryption, creating seamless customer experiences and in turn earning their loyalty and trust.

For more information visit www.echoworx.com

✉ info@echoworx.com
North America 1 800.346.4193 | UK 44 0.800.368.5334
@Echoworx